BayRS Version 15.3.0.0

Part No. 314470-15.3 Rev 00
April 2002

600 Technology Park Drive
Billerica, MA 01821-4130

BayRS Version 15.3.0.0 Document Change Notice

NORTEL NETWORKS™

Copyright © 2002 Nortel Networks

All rights reserved. April 2002.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, AN, ARN, ASN, BayRS, BCC, BN, Passport, and System 5000 are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

An asterisk after a name denotes a trademarked item.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. Software License Agreement

This Software License Agreement ("License Agreement") is between you, the end-user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel

Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Preface

Before You Begin x
Text Conventions x
Acronyms xi
Hard-Copy Technical Manuals xii
How to Get Help xii

Chapter 1
Configuring and Managing
Routers with Site Manager

Version 15.3.0.0 1-1
Changing the Trap Port for
Multiple Network Management Applications 1-1

Chapter 2
Configuring ATM Services

Version 15.2.0.0 2-1
Creating an ATM Circuit for a T3 or E3 Connection on a Passport 5430 2-1
Specifying the Cable Length 2-2
Specifying the Clear Alarm Threshold 2-2
Specifying the Line Coding Method 2-3
Specifying the Line Type 2-3
Specifying the Loopback Mode 2-3
Defining the Interface MTU 2-4
Defining the Primary Clock Source 2-4
Specifying the Setup Alarm Threshold 2-5
Disabling and Reenabling the ATM interface 2-5
Version 15.3.0.0 2-8
Defining the SVC Inactivity Timeout 2-8
Defining the Clocking Signal Source 2-10

Chapter 3
Configuring Bridging Services

Version 15.2.0.0 3-1
Interfaces Supported 3-1

Chapter 4
Configuring Differentiated Services

Version 15.1.0.0 4-1
Modifying RED Parameters 4-1
Version 15.2.0.0 4-2
Priority Parameter 4-2
Version 15.3.0.0 4-2
Implementation Notes 4-2

Chapter 5
Configuring Frame Relay Services

Version 15.1.0.0 5-1
Using Traffic Shaping – Site Manager 5-1
Version 15.2.0.0 5-2
Deleting PVCs from Service Records 5-2

Chapter 6
Configuring IP, ARP, RIP, RARP, and OSPF Services

Version 15.3.0.0 6-1
RFC826 Support 6-1

Chapter 7
Configuring IP Multicasting and Multimedia Services

Version 15.2.0.0 7-1
Configuring a PIM Bootstrap Border Router 7-1

Chapter 8
Configuring RADIUS

Version 15.2.0.0 8-1
Configuring a RADIUS Client Using Site Manager 8-1
Modifying Router Access Using the BCC or Site Manager 8-2
User/Manager Lock 8-2
Login Accounting 8-4

Using SecurID for RADIUS Authentication 8-5

Chapter 9
Using the Technician Interface Scripts

Version 15.1.0.0 9-1
Using Scripts and Aliases to Dynamically Configure a Router 9-1

Chapter 10
Using the Technician Interface Software

Version 15.1.0.0 10-1
Diagnostics On/Off Option for ARN, Passport 2340, and Passport 5430 10-1
Setting Default Route Cost Using the Technician Interface 10-1

Chapter 11
Configuring VRRP Services

Version 15.3.0.0 11-1
Enabling or Disabling VRRP Ping 11-1

Chapter 12
Quick-Starting Routers

Version 15.3.0.0 12-1
SPARCstation System Requirements 12-1
HP 9000 Workstation System Requirements 12-2

Chapter 13
Upgrading Routers to BayRS Version 15.*x*

Version 15.2.0.0 13-1
Why You Upgrade Boot and Diagnostic PROMs 13-1
Version 15.3.0.0 13-3
Site Manager Upgrade Prerequisites 13-3
Reviewing Site Manager System Requirements 13-3

Appendix A
Site Manager Parameters

ATM Port Parameters A-2
ATM Line Parameters A-5
Automated Security Association (IKE) Parameters A-9
Frame Relay PVC Parameter A-10
IP Global Parameter A-11

IP PIM Parameter A-12
NAT Global Parameter A-13
RADIUS Client Parameters A-14
RADIUS Access Control Parameters A-16
VRRP Parameter A-17

Preface

BayRS* Version 15.3.0.0 is a software release that includes bug fixes and new features added since BayRS Version 15.2.0.0. This document change notice contains amendments to the following BayRS manuals since BayRS Version 15.1.0.0:

- *Configuring and Managing Routers with Site Manager*
- *Configuring ATM Services*
- *Configuring Bridging Services*
- *Configuring Differentiated Services*
- *Configuring Frame Relay Services*
- *Configuring IP, ARP, RIP, RARP, and OSPF Services*
- *Configuring IP Multicasting and Multimedia Services*
- *Configuring RADIUS*
- *Configuring the Technician Interface Scripts*
- *Configuring the Technician Interface Software*
- *Configuring VRRP Services*
- *Quick-Starting Routers*
- *Upgrading Routers to BayRS Version 15.x*

Before You Begin

Before using this notice, you must complete the following procedures. For a new router:

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring Remote Access for AN and Passport ARN Routers*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Nortel Networks* BayRS and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: **ping** <*ip_address*>, you enter: **ping 192.32.10.12**
bold text	Indicates command names and options and text that you need to enter. Example: Enter **show ip** {**alerts** | **routes**}. Example: Use the **dinfo** command.
braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you must enter either: **show ip alerts** or **show ip routes**, but not both.

italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: **show at** <*valid_route*> *valid_route* is one variable and you substitute one value for it.
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

This guide uses the following acronyms:

ARN	Advanced Remote Node
ARP	Address Resolution Protocol
ATM	asynchronous transfer mode
FDDI	Fiber Distributed Data Interface
IP	Internet Protocol
MTU	maximum transmission unit
PBBI	PIM bootstrap border interface
PBBR	PIM bootstrap border router
PIM	Protocol Independent Multicast
PMC	PCI mezzanine card

PVC	permanent virtual circuit
RADIUS	Remote Access Dial-In User Services
SRB	source route bridge
VC	virtual circuit
VRRP	Virtual Router Redundancy Protocol

Hard-Copy Technical Manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

You can purchase selected documentation sets, CDs, and technical publications through the Internet at the www1.fatbrain.com/documentation/nortel/ URL.

How to Get Help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

Additional information about the Nortel Networks Technical Solutions Centers is available from the www.nortelnetworks.com/help/contact/global URL.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www130.nortelnetworks.com/cgi-bin/eserv/common/essContactUs.jsp URL.

Chapter 1
Configuring and Managing Routers with Site Manager

Version 15.3.0.0

The following section is an amendment to Chapter 7, "Monitoring Trap and Event Messages" in *Configuring and Managing Routers with Site Manager.*

Changing the Trap Port for Multiple Network Management Applications

If you are running more than one network management application on your Site Manager workstation, you must configure Site Manager to receive trap messages from the SNMP agent on a port other than the default port, 162. This is necessary for the following reasons:

- The agent can only send trap messages to one network management application at a time.
- Only one application can map to a UDP port at a time.

  By default, the network management application on your workstation is assigned to User Datagram Protocol (UDP) port 162. This port is dedicated to receiving SNMP trap messages from the SNMP agent.

  Site Manager is the preferred network management application for receiving trap messages. To avoid any problems when running another network management application, Nortel Networks recommends that you configure Site Manager to map to an alternative UDP port. This allows you to send trap messages to Site Manager directly.

To reconfigure the trap port:

1. **In the Configuration Manager window, choose Protocols > IP > SNMP > Communities.**

   The SNMP Community List window opens.

2. **Choose Community > Managers.**

   The SNMP Manager List window opens.

3. **Choose Manager > Edit Manager.**

   The Trap Port and Trap Types window opens.

4. **Type a new port number for the Trap Port parameter, then click on OK.**

   You can enter any port number on your Site Manager workstation, as long as another application is not using that port.

   You return to the Configuration Manager window.

5. **Choose File > Save to save this configuration file.**

   See Chapter 3 in *Configuring and Managing Routers Using Site Manager* for instructions on saving configuration files.

6. **Choose File > Exit.**

   You return to the main Site Manager window.

7. **Restart Site Manager according to the instructions in Chapter 1 of *Configuring and Managing Routers Using Site Manager***

   To make sure that Site Manager is able to listen to the port that you configured in step 4, restart Site Manager using the **wfsm -e** command or the Trap Monitor using the **wftraps -e** command. For more information, about using the **wfsm** and **wftraps** commands with the **-e** option, see Appendix A in *Configuring and Managing Routers with Site Manager.*

Note: You can also change the trap port on a PC by editing the snmp-trap 162/udp snmp string in the Services file. From the Start menu, choose **Programs** > **Windows Explorer**. Open the Services file and edit the string snmp-trap 162/udp snmp. For example, to change the trap port from 162 to 779, enter **snmp-trap 779/udp snmp** and reboot the PC. Site Manager PC is then able to receive the traps from the router on port 779.

Chapter 2
Configuring ATM Services

Version 15.2.0.0

The following section is new to *Configuring ATM Services*. You use the procedures in this section to configure an ATM T3/E3 PMC module installed in a Passport* 5430. For information about installing an ATM T3/E3 PMC module, see *ATM T3/E3 PMC Module Supplement*.

Creating an ATM Circuit for a T3 or E3 Connection on a Passport 5430

To start ATM services on an ATM T3/E3 PMC module in the Passport 5430, you do the following:

1. Configure the physical ATM circuit.
2. Add protocols and other services to that circuit.

This section describes how you create a physical ATM circuit for a T3 or E3 connection on a Passport 5430, then directs you to *Configuring ATM Services* for information about adding protocols and further configuring ATM services.

Using the BCC

To add ATM to a Passport 5430 with a T3/E3 connector, navigate to the box prompt and enter:

atm slot <*slot_number*> **pci-slot** <*pci_slot*> **module** <*module_number*> **connector** <*connector_number*> **mode** {**t3** | **e3**}

slot_number is the number of the chassis slot containing the ATM T3/E3 PMC module.

pci_slot is the number of the PCI slot containing the ATM T3/E3 PMC module. The PCI slot number for the ATM T3/E3 PMC module is always 1.

module_number is always 2 for the ATM interface.

connector_number is the number of a connector on the ATM T3/E3 PMC module.

mode t3 or **mode e3** specifies whether the ATM interface is a T3 or E3 interface.

For example, the following command adds an ATM T3 interface to the Passport 5430 configuration on slot 1, PCI slot 1, module 2, connector 1:

```
box# atm slot 1 pci-slot 1 module 2 connector 1 mode t3
atm/1/1/2/1#
```

To configure T3/E3 parameters, use the following procedures.

Specifying the Cable Length

To specify the cable length, navigate to the ATM interface prompt (for example, **box**; **atm/1/1/2/1**; **atm-e3**) and enter:

cable-length <*length*>

length is either short (default) or long. Specify short for a cable less than 225 feet long; specify long for a cable length of 225 feet or more.

For example, the following command changes the cable length to long:

```
atm-e3/1/1/2/1# cable-length long
atm-e3/1/1/2/1#
```

Specifying the Clear Alarm Threshold

To specify the duration of time (in seconds) that elapses following the clearing of a performance failure (before the condition is registered and logged), navigate to the ATM interface prompt (for example, **box**; **atm/1/1/2/1**; **atm-e3**) and enter:

clear-alarm-threshold <*integer*>

integer is a value from 2 through 10 seconds, inclusive.

For example, the following command changes the clear alarm threshold from 2 to 8 seconds:

```
atm-e3/1/1/2/1# clear-alarm-threshold 8
atm-e3/1/1/2/1#
```

Specifying the Line Coding Method

To specify the line coding method, navigate to the ATM interface prompt (for example, **box**; **atm/1/1/2/1**; **atm-e3**) and enter:

line-coding {hdb3 | b3zs}

The default for the ATM E3 interface is hdb3 and the default value for the ATM T3 interface is b3zs.

Specifying the Line Type

To specify the line type for this interface, navigate to the ATM interface prompt (for example, **box**; **atm/1/1/2/1**; **atm-e3**) and enter:

line-type <*type*>

type is autodetect, ds3m23, or ds3cbitparity for the ATM T3 interface and e3framed or e3plcp for the ATM E3 interface.

If the line type is ds3m23, the framing mode should be m23 or t3m23plcp.

If the line type is ds3cbitparity, the framing mode should be cbit or t3cbitplcp.

If the line type is either e3framed or e3plcp, the framing mode should be either g751or g832.

For instructions on setting the framing-mode parameter, see *Configuring ATM Services.*

Specifying the Loopback Mode

To force the interface into loopback mode so that the far-end or intermediate equipment can perform diagnostics on the network between that equipment and the T3/E3 interface, navigate to the ATM interface prompt (for example, **box**; **atm/1/1/2/1**; **atm-e3**) and enter:

loopback-mode <*type*>

type is payloadloop or lineloop.

If you select payloadloop, the received signal at this interface is looped through the device. Typically, the received signal is looped back for retransmission after it has passed through the device's framing function.

If you select lineloop, the received signal at this interface does not go through the framing device (minimum penetration) but is looped back out. The default is noloop.

For example, the following command changes the loopback mode to payloadloop:

```
atm-e3/1/1/2/1# loopback-mode payloadloop
atm-e3/1/1/2/1#
```

Defining the Interface MTU

The maximum transmission unit (MTU) is the largest possible unit of data that the physical medium can transmit. By default, the interface allows an MTU size of 4608 octets. This value can handle most packet sizes. However, you can set the MTU to any value from 3 through 4608 octets.

To modify the interface MTU, navigate to the ATM interface prompt (for example,
box; **atm/1/1/2/1**; **atm-e3**) and enter:

mtu <*integer*>

integer is the MTU size in octets.

For example, the following command sets the MTU size to 3000 octets:

```
atm-e3/1/1/2/1# mtu 3000
atm-e3/1/1/2/1#
```

Defining the Primary Clock Source

To define the clock signal source, navigate to the ATM interface prompt (for example, **box**; **atm/1/1/2/1**; **atm-e3**) and enter:

primary-clock-source <*value*>

value is internal or loop. If you select internal, the router will generate the clock signal source. If you select the default, loop, the clock signal source will be external to the router.

For example, the following command sets the clock source to internal:

```
atm-e3/1/1/2/1# primary-clock-source internal
atm-e3/1/1/2/1#
```

Specifying the Setup Alarm Threshold

To specify the duration of time (in seconds) that elapses following the detection of a performance failure, before the condition is registered and logged, navigate to the ATM interface prompt (for example, **box**; **atm/1/1/2/1**; **atm-e3**) and enter:

setup-alarm-threshold <*integer*>

integer is a value from 2 through 10 seconds, inclusive.

For example, the following command changes the setup alarm threshold from 2 to 8 seconds:

```
atm-e3/1/1/2/1# setup-alarm-threshold 8
atm-e3/1/1/2/1#
```

Disabling and Reenabling the ATM interface

By default, the ATM interface is enabled when you create the circuit. However, you can disable or reenable the interface at any time. When the interface is enabled, traffic can flow over the interface. When the interface is disabled, traffic cannot flow over the interface.

To disable or reenable the ATM interface, navigate to the ATM interface prompt (for example, **box**; **atm/1/1/2/1**; **atm-e3**) and enter:

state {**disabled** | **enabled**}

For example, the following commands disable and reenable the ATM interface:

```
atm-e3/1/1/2/1# state disabled
atm-e3/1/1/2/1# state enabled
atm-e3/1/1/2/1#
```

Using Site Manager

To create an ATM circuit for a T3 or E3 connection on a Passport 5430, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the ATM DS3/E3 interface (**ATM1**) in slot 1, PCI slot 1, module 2.	The Add Circuit window opens.
2. Click on **OK** to accept the default circuit name.	The ATM Configuration window opens.
3. Click on **Physical Layer Configuration**.	The Physical Layer Configuration window opens.
4. Click on either **DS3** or **E3**.	The Port Parameters window opens.
5. To configure port parameters, set the following parameters as needed: • **Enable/Disable** • **Line Type** • **Setup Alarm Threshold (seconds)** • **Clear Alarm Threshold (seconds)** • **Loopback Configuration** • **Primary Clock** Click on **Help** or see the parameter descriptions in "ATM Port Parameters," beginning on page A-2.	
6. Click on **OK**.	The Physical Layer Configuration window opens.
7. Click on **Done**.	The ATM Configuration window opens.
8. Click on **ATM Line Attributes.**	The ATM Line Driver Attributes window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
9. Set the the following parameters as needed: • **Enable** • **Interface MTU** • **Data Path Enable** • **Data Path Notify Timeout** • **Framing Mode** • **Cell Scrambling** • **Per-VC Clipping** • **DS3 Line Build Out** Note: The **Cell Scrambling** parameter value must be the same as for the other ATM devices on your network. See your system administrator or your service provider for the appropriate value. Click on **Help** or see the parameter descriptions in “ATM Line Parameters” on page A-5.	
10. Click on **OK.**	The ATM Configuration window opens.
11. Click on **ATM**.	The Edit ATM Connector window opens.
12. Go to “Defining an ATM Service Record” in *Configuring ATM Services*.	

After you create the ATM circuit, go to Chapter 2, “Starting ATM and ATM Router Redundancy,” in *Configuring ATM Services* to finish configuring ATM services.

Configuring ATM Services also provides more information about ATM services and how to modify an existing ATM configuration.

Version 15.3.0.0

The following sections contain amendments to Chapter 3, “Customizing an ATM Interface” in *Configuring ATM Services*.

Defining the SVC Inactivity Timeout

When you enable the SVC inactivity timeout function (the default), the router automatically terminates any SVCs that have not received or transmitted any cells. If you disable the SVC inactivity timeout function, all SVCs on the line remain open until you close them by another method.

When enabled, the SVC inactivity timeout function also requires a timer value. This timer value specifies how long you want the ATM router to wait before disabling inactive SVCs. By default, if the router does not receive or transmit any cells for 1200 seconds, the inactive SVCs are disabled. However, you can set this timer to any value from 60 to 3600 seconds.

Using the BCC

To disable the SVC inactivity timeout function, navigate to the ATM prompt (for example, **box; atm/11/1**) and enter:

vc-inactivity-control disabled

For example, the following command disables the SVC inactivity timeout function on the ATM interface:

```
atm/11/1# vc-inactivity-control disabled
atm/11/1#
```

To reenable the SVC inactivity timeout function, navigate to the ATM prompt and enter:

vc-inactivity-control enabled

Note: The **vc-inactivity-control** parameter is not available for use with the ATM T3/E3 PMC module. Instead, the **vc-inact-control** parameter appears for this module. The **vc-inact-control** parameter cannot be modified.

To change the SVC inactivity timeout value, navigate to the ATM prompt and enter:

vc-inactivity-timeout <*integer*>

integer is the amount of time (in seconds) that the router waits before it disables inactive SVCs.

For example, the following command sequence reenables the SVC inactivity timeout function on the ATM interface and sets the SVC inactivity timeout value to 2400 seconds:

```
atm/11/1# vc-inactivity-control enabled
atm/11/1# vc-inactivity-timeout 2400
atm/11/1#
```

Note: The **vc-inactivity-timeout** parameter is not available for use with the ATM T3/E3 PMC module. Instead, the **vc-inact-timeout** parameter appears for this module. The **vc-inact-timeout** parameter cannot be modified.

Defining the Clocking Signal Source

You can specify either an internal or external clocking source for time signals. Internal clocking uses the router clock; external clocking uses the line clock.

Using the BCC

To change the source of the ATM clocking signal, navigate to the ATM prompt (for example, **box; atm/11/1**) and enter:

clock-signal-source <*source*>

source is either internal (default) or external.

For example, the following command changes the ATM clocking signal source to external:

```
atm/11/1# clock-signal-source external

atm/11/1#
```

Note: The **clock-signal-source** parameter is not available for use with the ATM T3/E3 PMC module. Instead, the **clk-signal-source** parameter appears for this module. The **clk-signal-source** parameter cannot be modified.

Chapter 3
Configuring Bridging Services

Version 15.2.0.0

The following section corrects erroneous text in *Configuring Bridging Services*.

Interfaces Supported

The section “Interfaces Supported” under “Implementation Notes” in *Configuring Bridging Services* incorrectly states that the translation bridge can operate on all SR interfaces supported by Nortel Networks routers except IP. The translation bridge can operate on all SR interfaces supported by Nortel Networks routers except for interfaces configured for SRB with IP encapsulation.

Chapter 4
Configuring Differentiated Services

Version 15.1.0.0

The following section describes a change to *Configuring Differentiated Services.*

Modifying RED Parameters

The following change is required to Table 6-1 in the "Modifying RED Parameters" section of the *Configuring Differentiated Services* book.

The proper range of values for the **id** parameter is from 1 through 65535. The proper range is shown in the following table, which lists RED parameters that can be configured under **dsqms-red**, their values, and functions.

Parameter	Values	Function
id	integer 1 through 65535	Identifies the RED function. You cannot change this parameter.
min-threshold	integer 0 through 100 (default 20)	Indicates the queue size below which no packets are dropped by RED
max-threshold	integer 1 through 100 (default 80)	Indicates the queue size above which all packets are dropped by RED
first-order-const	integer 0 through 100 (default 1)	Specifies the first order constant used when calculating drop probability based on the average queue fraction, the queue size, and the min-threshold value
second-order-const	integer 0 through 1000 (default 10)	Specifies the second order constant used when calculating drop probability based on the average queue fraction, the queue size, and the min-threshold value

Version 15.2.0.0

The following section corrects erroneous text in the description of the Priority parameter.

Priority Parameter

The description of the Priority parameter in Appendix A incorrectly states that the lower the number, the higher the priority. The description should state that the higher the number, the higher the priority. For example, a server with a priority of 2 will be the active server before a server with a priority of 1.

Version 15.3.0.0

The following section is an amendment to Chapter 2, “Starting Differentiated Services” in *Configuring Differentiated Services*.

Implementation Notes

The following guidelines can help you successfully configure DSQMS on your router:

- You can configure DSQMS on these interfaces only: HSSI, MCT1, MCE1, T1/FT1, E1/FE1, and synchronous.
- If you enable flow fairness on a queue, you cannot configure that queue as a best-effort queue. For information about enabling flow fairness on a queue or designating the queue as best effort, see “Modifying a DSQMS Queue” in *Configuring Differentiated Services*.
- If you configure both weighted and priority queues on an interface, you may experience latency problems with the highest priority queues. To avoid such problems:
  - -- Set the DSQMS interface parameter **dequeue-at-line-rate** to **enabled** (the default value is **disabled**). See “Configuring DSQMS to Dequeue Packets at Line Rate” in *Configuring Differentiated Services* for instructions.
  - -- Ensure that the amount of high-priority traffic is not excessive in the highest priority queues.

- If you implement RED for queue management instead of tail-drop (that is, you set the queue parameter **drop-type** to **red** and you associate the queue classifier with a RED function), the probability of dropping packets may adversely affect the latency requirements of some applications. Adjust the following parameters to achieve the required latency levels for the queue:
  - -- RED parameters **min-threshold** and **max-threshold** (see "Modifying RED Parameters" on page 3-1 for instructions).
  - -- Queue parameters **average-queue-gain** and **idle-queue-loss-rate** (see "Modifying a DSQMS Queue" in *Configuring Differentiated Services* for instructions).

Chapter 5
Configuring Frame Relay Services

Version 15.1.0.0

The following changes are required to the *Configuring Frame Relay Services* book.

A new frame relay parameter, Bw Threshold, has been added to the PVC List for Services window in Site Manager. The Bw Threshold parameter works in conjunction with the Committed Burst, Excess Burst, and Throughput parameters to shape traffic.

The following sections update the Site Manager procedure within the "Using Traffic Shaping" section in Chapter 4 and adds the parameter description to Appendix A: "Site Manager Parameters."

Using Traffic Shaping – Site Manager

To enable traffic shaping, complete the following tasks using Site Manager:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Select the appropriate service record and click on **PVCs**.	The FR PVC List for Service window opens.
5. Click on a PVC that you want to configure for traffic shaping.	
6. Set the following parameters: • **Committed Burst** • **Excess Burst** • **Throughput** • **Bw Threshold** Click on **Help** or see the parameter description in "Frame Relay PVC Parameter" on page A-10.	
7. Click on **Done**.	You return to the Frame Relay Service List window.
8. Click on **Done**.	You return to the Frame Relay Circuit Definition window.
9. Click on **Done**.	You return to the Configuration Manager window.

Version 15.2.0.0

The following section describes a limitation that was omitted from *Configuring Frame Relay Services*.

Deleting PVCs from Service Records

The section "Deleting PVCs from Service Records" in *Configuring Frame Relay Services* should include the statement that Site Manager does not allow users to delete or move the last PVC in the only non-default service record. If you want to delete or move the last PVC, you must remove the entire service record.

Chapter 6
Configuring IP, ARP, RIP, RARP, and OSPF Services

Version 15.3.0.0

The following section is new to Chapter 1, “IP Concepts, Terminology, and Features” in *Configuring IP, ARP, RIP, RARP, and OSPF Services*.

RFC826 Support

BayRS now supports RFC826: An Ethernet Address Resolution Protocol. According to RFC826, when a router interface receives an ARP request or reply, it checks the source IP address to make sure that it is valid and the router’s translation table for the destination IP and MAC address pair. If the saved MAC address in the table is different from the reported MAC address, the router replaces the old MAC address with the new one. The interface then checks for the message type (request or reply). If the router cannot find the MAC address in the translation table, it discards the message.

Chapter 7
Configuring IP Multicasting and Multimedia Services

Version 15.2.0.0

The following section is new to *Configuring IP Multicasting and Multimedia Services*.

Configuring a PIM Bootstrap Border Router

You can define a router as a PIM bootstrap border router (PBBR) by specifying at least one of its interfaces as a PIM bootstrap border interface (PBBI). A bootstrap border router prevents a bootstrap message that is received from one side of a border router from being passed to the other side of the router. The bootstrap border router allows you to create two or more PIM bootstrap domains in one PIM domain so that the rendezvous point (RP) information kept in the routers can be different.

To specify a PIM bootstrap router as a border router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **PIM**.	The PIM menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Choose **Interface**.	The PIM Interface Parameters window opens.
5. Set the **Bootstrap Border** parameter. Click on **Help** or see the parameter description in “IP PIM Parameter” on page A-12.	
6. Click on **OK**.	You return to the Configuration Manager window.

Chapter 8
Configuring RADIUS

Version 15.2.0.0

The following sections are amendments to *Configuring RADIUS*:

Topic	Page
Configuring a RADIUS Client Using Site Manager	8-1
Modifying Router Access Using the BCC or Site Manager	8-2
Using SecurID for RADIUS Authentication	8-5

Configuring a RADIUS Client Using Site Manager

With earlier versions of Site Manager, you configured RADIUS only on link modules that had synchronous interfaces. With Version 15.2.0.0, you can use Site Manager to configure RADIUS on any link module, including Quad Ethernet, FDDI, and token ring. Consequently, Site Manager no longer automatically configures a demand circuit group when you use it to configure a RADIUS client.

To enable RADIUS on a router slot and configure the RADIUS client:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, select **Protocols > Global Protocols > RADIUS > Create RADIUS**.	The RADIUS Client Parameters window opens. The window lists the slots that already have RADIUS configured on them.
2. Click on **Add**.	For multislot routers, the RADIUS Slot Selection window opens. For single-slot routers, the RADIUS Client Parameters window opens. Go to step 4.
3. Enter the slot number on which you want to configure RADIUS and click on **OK**.	The RADIUS Client Parameters window opens.
4. Set the following parameters: • **Authentication** • **Accounting** • **Client IP Address** • **Debug Message Level** Click on **Help** or see the parameter descriptions beginning on page A-14.	
5. Click on **OK**.	You return to the RADIUS Client Parameters window.

Modifying Router Access Using the BCC or Site Manager

With RADIUS, you can modify access to the router using the user/manager lock and the login accounting feature.

User/Manager Lock

With earlier versions of BayRS, you enabled the user/manager lock using the Technician Interface only. You can now enable it using the BCC or Site Manager. The lock is disabled by default, allowing access by all users with the user or manager profile, and also by individual users with a unique profile. You enable the lock when both the RADIUS client and server are available. You disable the lock if the RADIUS server is not available, allowing the user to log in with the manager or user profile.

When you enable the user/manager lock and a RADIUS server is unavailable for authentication, the router automatically disables the user/manager lock. When the RADIUS server becomes available, the router automatically enables the user/manager lock.

Note: Be sure to configure RADIUS and assign the appropriate access to individuals with unique profiles before you enable the user/manager lock; otherwise you may lock out system managers from the router.

Using the BCC

To restrict access to individual users only, navigate to the access prompt (for example, **box; access**) and enter:

user-manager-lock enable

To allow access by all users with the manager or user profile, in addition to users with a unique profile, navigate to the access prompt (for example, **box; access**) and enter:

user-manager-lock disable

Using Site Manager

To restrict access to individual users only, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols > Global Protocols > RADIUS > Access Control**.	The RADIUS Access Control window opens.
2. Set the **User Manager Lock** parameter to **Enable**. For more information, click on **Help** or see the parameter descriptions beginning on page A-16.	
3. Click on **OK**.	You return to the Configuration Manager window.

Login Accounting

BayRS RADIUS accounting is now supported for console and Telnet router logins. The following sections, new to *Configuring RADIUS*, describe the functionality that was added to support this feature.

You determine whether a console or Telnet login session should allow RADIUS accounting messages to be sent to the RADIUS server by enabling or disabling RADIUS accounting access to the server.

Using the BCC

To allow RADIUS accounting messages to be sent to the RADIUS server, navigate to the access prompt (for example, **box; access**) and enter:

user-access-radius-account-enable enable

To prevent RADIUS accounting messages from being sent to the RADIUS server, navigate to the access prompt (for example, **box; access**) and enter:

user-access-radius-account-enable disable

Note: If you enable login accounting, and the RADIUS server becomes unavailable, the value for the **user-access-radius-account-enable** parameter is automatically set to “serverwait.” When the RADIUS server becomes available again, the value reverts to enabled.

Using Site Manager

To allow RADIUS accounting messages to be sent to the RADIUS server, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols > Global Protocols > RADIUS > Access Control**.	The RADIUS Access Control window opens.
2. Set the **Login Accounting** parameter to **Enable**. For more information, click on **Help** or see the parameter descriptions beginning in page A-16.	
3. Click on **OK**.	You return to the Configuration Manager window.

Using SecurID for RADIUS Authentication

This section in *Configuring RADIUS* incorrectly states that Nortel Networks implements SecurID on ARN* routers only. Nortel Networks implements SecurID on all router platforms that operate as RADIUS clients.

Chapter 9
Using the Technician Interface Scripts

Version 15.1.0.0

The Technician Interface is a command-line interface that Nortel Networks support technicians can use to troubleshoot and configure Nortel Networks devices.

The following section is an amendment to *Using the Technician Interface Scripts*:

Using Scripts and Aliases to Dynamically Configure a Router

Use of rapid-fire scripts or aliases to dynamically set a router's configuration via the MIBs can put the router into a corrupted state and cause connectivity issues. When you use the Technician Interface to launch scripts or aliases to configure the router be sure to include pauses (one to two seconds) to allow sufficient time for the router to make the required changes to the MIBs.

Chapter 10
Using the Technician Interface Software

Version 15.1.0.0

The Technician Interface is a command-line interface that Nortel Networks support technicians can use to troubleshoot and configure Nortel Networks devices.

The following sections are amendments to *Using the Technician Interface Software*:

Diagnostics On/Off Option for ARN, Passport 2340, and Passport 5430

For ARN, Passport 2430 and Passport 5430 platforms *only,* the Technician Interface **diags** command supports an option to enable or disable diagnostics, effective the next time you cycle power on the router. Disabling the diagnostics results in a faster boot time, but leaves the hardware components unverified. The syntax for this option is as follows:

diags [**- on|off**] [<*slot_id*>]

Setting Default Route Cost Using the Technician Interface

When the routing table does not contain the route to a particular destination address, the router looks for a default route. As it does for any other route, the routing table either acquires the default route dynamically (through a routing protocol), or you can enter the default route statically.

You can use the Technician Interface to set the wfRipIntfDefaultRouteCost (RIP default route cost) MIB attribute. This attribute interacts with the Site Manager parameter Default Route Supply or BCC parameter default-supply in one of two ways:

- If you select Enable for Default Route Supply or default-supply, RIP advertises the default route cost you set for wfRipIntfDefaultRouteCost attribute *plus* the default route learned from the network.
- If you select Generate for Default Route Supply or default-supply, RIP advertises the default route cost you set for wfRipIntfDefaultRouteCost.

For additional information, see "Supplying a Default Route on an Interface" in *Configuring IP, ARP, RARP, RIP and OSPF Services*.

With the Technician Interface, enter the following commands to set the wfRipIntfDefaultRouteCost (RIP default route cost) attribute:

set wfRipIntfDefaultRouteCost <*value*>

value is any integer from 0 through 15. The default value is 1.

commit

save config <*vol*>*:* <*filename*>

You must have Manager access to issue a **set** command. The **commit** command causes the changes you made to the configuration to take effect in active memory, but not in flash memory. The **save config** command saves changes to a configuration file (config) and flash volume on the router.

Chapter 11
Configuring VRRP Services

Version 15.3.0.0

The following section is new to Chapter 3, “Customizing VRRP” in *Configuring VRRP Services*.

Enabling or Disabling VRRP Ping

When enabled, this feature allows you to ping a master virtual router that is not the owner of the virtual IP address. By default, VRRP ping is disabled.

Using the BCC

To enable VRRP ping, access the virtual router (for example, **box; ip; vrrp 192.41.31.21/2 vr-ip-address 192.41.31.22**) and enter:

ping-enable enabled

To disable VRRP ping, access the virtual router and enter:

ping-enable disabled

For example, to enable VRRP ping, enter the following command:

```
vrrp/192.41.31.21/2# ping-enable enabled
vrrp/192.41.31.21/2#
```

Using Site Manager

To enable VRRP ping, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted router appears.
5. Set the **VRRP Address Ping** parameter. Click on **Help** or see the parameter description on page A-17.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Chapter 12
Quick-Starting Routers

Version 15.3.0.0

The following section contains an amendment to Chapter 10, “Installing Site Manager on a SPARCstation” in *Quick-Starting Routers*.

SPARCstation System Requirements

To run Site Manager, your SPARCstation must meet the following hardware and software requirements:

- Supported workstations:
  - -- SPARCstation 10, 20
  - -- UltraSPARC
- Supported operating systems: Solaris 2.7 and 2.8
- Window environment:
  - -- CDE 1.0.1
  - -- OpenWindows 3.5
- 32 MB of RAM (64 MB recommended)
- 145 MB of disk space
- 32 MB of swap space
- Network adapter appropriate for your network
- CD-ROM drive

The following section contains an amendment to Chapter 12, Installing Site Manager on an HP 9000 Workstation in *Quick-Starting Routers*.

HP 9000 Workstation System Requirements

To run Site Manager, your HP 9000 workstation must meet the following hardware and software requirements:

- Supported workstations: HP 9000 Series 700 and 800
- Supported operating systems: HP-UX 10.20 (BayRS Version 15.3.0.0 or greater) and HP-UX 11.00, including the complete services (network services) directory
- Window environment: CDE 1.0.1
- 32 MB of RAM
- 145 MB of free disk space
- 32 MB of swap space (64 MB recommended)
- Network adapter appropriate for your network
- CD-ROM drive

Chapter 13
Upgrading Routers to BayRS Version 15.*x*

Version 15.2.0.0

The following section describes changes to *Upgrading Routers to BayRS Version 15.x*.

Why You Upgrade Boot and Diagnostic PROMs

Table A-1 in "Why You Upgrade Boot and Diagnostic PROMs" of *Upgrading Routers to BayRS Version 15.x* has been modified to include the latest boot and diagnostic PROM file names and associated revision numbers for router platforms running BayRS Version 15.*x*.

Router Platform	Diagnostic PROM File Name	Diagnostic PROM Revision Number	Reason for Upgrading PROM	Boot PROM File Name	Boot PROM Revision Number
AN/ANH*	andiag.exe	7.36	Strata flash feature support	anboot.exe	9.00d
ARN	arndiag.exe	2.24	Strata flash feature support	arnboot.exe	1.27
	arndiag.rom	2.24	Not applicable	arnboot.rom	1.27
	e7srom.rom	2.16	E7S feature support	isdb.rom	1.06
	arn_pdbrom.rom	1.22	Not applicable		

Router Platform	Diagnostic PROM File Name	Diagnostic PROM Revision Number	Reason for Upgrading PROM	Boot PROM File Name	Boot PROM Revision Number
ASN*	asndiag.exe	2.36	Strata flash feature support	asnboot.exe	13.00
	asndiag.rom	2.36	Not applicable		
BN*	frediag.exe	5.16	Strata flash feature support	freboot.exe	13.00
	fre4diag.ppc	1.14	FRE-4 board support	fre4boot.ppc	13.20
ARE (BN, 5782 MPE)	arediag.ppc	1.22	Strata flash feature support	areboot.ppc	14.0.1.0
Passport 2430	pp2430diag.exe	2.06	Not applicable	pp2430boot.ppc	14.10
	pp2430ram.exe	2.06	Not applicable		
	pp2430diag.a	2.06	Not applicable		
Passport 5430	pp5430diag.exe	1.10	Not applicable	pp5430boot.ppc	15.2.0.0
	pp5430ram.exe	1.10	Not applicable		
	pp5430diag.a	1.10	DS3/E3 feature support and quad serial feature support		
System 5000* net modules	s5000diag.exe	0.04	Strata flash feature support	s5000boot.exe	13.00

Version 15.3.0.0

The following section describes changes to *Upgrading Routers to BayRS Version 15.x*.

Site Manager Upgrade Prerequisites

Before you upgrade to Site Manager Version 15.*x*, review Site Manager system requirements.

Reviewing Site Manager System Requirements

Site Manager is a graphical user interface (GUI) for router configuration and management over an IP network. To run Site Manager Version 15.*x*, your PC, IBM* workstation, SPARCstation*, or HP* 9000 must meet the hardware and software requirements listed in Table 13-1.

Table 13-1. Site Manager System Requirements

Platform	Hardware and Software Requirements
PC	• 486 PC (Pentium recommended) • Microsoft* Windows* 98 or 2000 (32-bit) or Windows NT* Version 4.0 (32-bit) • 16 MB of RAM (minimum) • 90 MB of free disk space • Microsoft TCP/IP for Windows 98 or 2000 and compatible network adapter and driver • CD-ROM drive • VGA monitor (SuperVGA monitor recommended)
SPARCstation	• Supported workstations: SPARCstation 10, 20, and UltraSPARC • Supported operating system: Solaris 2.7 and 2.8 • Window environments: CDE 1.0.1 and OpenWindows 3.5 • 32 MB of RAM (64 MB recommended) • 145 MB of disk space • 32 MB of swap space • Network adapter appropriate for your network • CD-ROM drive

Table 13-1. Site Manager System Requirements *(continued)*

Platform	Hardware and Software Requirements
IBM workstation	• Supported workstations: RS/6000 340, 370, and PowerPC • Supported operating system: IBM AIX* Version 4.3 • Window environments: CDE 1.0.1 and AIX Motif 1.2 • 32 MB of RAM (64 MB recommended) • 140 MB of disk space • 32 MB of swap space (64 MB recommended; use 96 MB of swap space with the NetView for AIX application) • Network adapter appropriate for your network • CD-ROM drive
HP 9000	• Supported workstations: HP 9000 Series 700 and 800 • Supported operating system: HP-UX 10.20 (BayRS Version 15.3.0.0 or greater) and HP-UX 11.00, including the complete network services directory • Window environment: CDE 1.0.1 • 32 MB of RAM • 145 MB of free disk space • 32 MB of swap space (64 MB recommended) • Network adapter appropriate for your network • CD-ROM drive

Appendix A
Site Manager Parameters

This appendix describes the following Site Manager parameters:

Topic	Page
ATM Port Parameters	A-2
ATM Line Parameters	A-5
Automated Security Association (IKE) Parameters	A-9
Frame Relay PVC Parameter	A-10
IP Global Parameter	A-11
IP PIM Parameter	A-12
NAT Global Parameter	A-13
RADIUS Client Parameters	A-14
RADIUS Access Control Parameters	A-16
VRRP Parameter	A-17

You can display the same information using Site Manager online Help.

For each parameter, this appendix provides the following information:

- Parameter name
- Configuration Manager menu path
- Default setting
- Valid parameter options
- Parameter function
- Instructions for setting the parameter

- Management information base (MIB) object ID

You can also use the Technician Interface to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is the same as modifying parameters using Site Manager. For information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

ATM Port Parameters

You use the following parameters to configure the ATM T3/E3 interface on the Passport 5430.

Parameter:	**Enable/Disable**
Path:	Configuration Manager > ATM1 > Physical Layer Configuration > **DS3** or **E3**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables this interface.
Instructions:	Set to Disable only if you want to disable the interface.
MIB Object ID:	1.3.6.1.4.1.18.3.4.26.10.1.2

Parameter: **Line Type**

Path: Configuration Manager > ATM1 > Physical Layer Configuration > **DS3** or **E3**

Default: Autodetect

Options: For DS3, the options are DS3 M23 | DS3 CBIT Parity | Autodetect

For E3, the options are E3 Framed | E3 PLCP

Function: Sets the frame format for this interface.

Instructions: Determines the framing mode for this interface.
For DS3, if you choose DS3 M23 or DS3 CBIT Parity, be sure that the ATM line attribute Framing Mode is appropriately set:

If the Line Type is DS3 M23, Framing Mode should be DS3_M23 or T3M23PLCP.

If Line Type is DS3 CBIT Parity, Framing Mode should be DS3_CBIT or T3CBITPLCP.

For E3, make sure that the ATM line attribute Framing Mode is set to either E3_G751 or E3_G832.

MIB Object ID: 1.3.6.1.4.1.18.3.4.26.10.1.7

Parameter: **Setup Alarm Threshold (seconds)**

Path: Configuration Manager > ATM1 > Physical Layer Configuration > **DS3** or **E3**

Default: 2

Options: 2 to 10

Function: Sets the time interval (in seconds) during which the device driver tolerates a performance defect or anomaly. If the performance defect or anomaly is still present when time interval expires, the device driver records a performance failure and logs an event message.

Instructions: Set the timer value in seconds.

MIB Object ID: 1.3.6.1.4.1.18.3.4.26.10.1.17

Parameter: **Clear Alarm Threshold (seconds)**

Path: Configuration Manager > ATM1 > Physical Layer Configuration > **DS3** or **E3**

Default: 2

Options: 2 to 10

Function: Specifies the clear time (in seconds) for performance failure conditions. If the defect or anomaly clears within this interval, the device driver records a performance cleared condition and logs an event message.

Instructions: Set the timer value in seconds.

MIB Object ID: 1.3.6.1.4.1.18.3.4.26.10.1.18

Parameter: **Loopback Configuration**

Path: Configuration Manager > ATM1 > Physical Layer Configuration > **DS3** or **E3**

Default: No Loopback

Options: No Loopback │ Payload Loopback │ Line Loopback

Function: Forces the interface into loopback mode. The far-end or intermediate equipment then performs diagnostics on the network between that equipment and the T3/E3 interface. After testing, set this parameter to No Loopback to return the interface to a normal operating mode.

- No Loopback — Returns the interface to non-loopback operation.
- Payload Loopback — The received signal at this interface is looped through the device. Typically the received signal is looped back for re-transmission after it has passed through the device's framing function.
- Line Loopback — The received signal at this interface does not go through the framing device (minimum penetration) but is looped back out.

Instructions: Select the loopback configuration option.

MIB Object ID: 1.3.6.1.4.1.18.3.4.26.10.1.9

Parameter: **Primary Clock**

Path: Configuration Manager > ATM1 > Physical Layer Configuration > **DS3** or **E3**

Default: Loop

Options: Internal | Loop

Function: Specifies the clock signal source.

Instructions: Select Internal if you want the router to generate the clock signal source. Otherwise, accept the default, Loop, if you want the clock signal source to be external to the router.

MIB Object ID: 1.3.6.1.4.1.18.3.4.26.10.1.11

ATM Line Parameters

You use the following parameters to configure ATM line details on the Passport 5430. The type of ATM link module you use determines the line details that you can edit.

Parameter: **Enable**

Path: Configuration Manager > ATM1 > ATM Line Attributes

Default: Enable

Options: Enable | Disable

Function: Enables or disables the line driver.

Instructions: Select Enable or Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.3.2.1.2

Parameter: **Interface MTU**

Path: Configuration Manager > ATM1 > ATM Line Attributes

Default: 4608

Options: 0 to 9188

Function: Specifies the largest packet size (in octets) that the router can transmit on this interface.

Instructions: Enter a value that is appropriate for the network.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.3.2.1.9

Parameter: Data Path Enable

Path: Configuration Manager > ATM1 > ATM Line Attributes

Default: Enable

Options: Enable | Disable

Function: Specifies whether the router disables the interface between the driver and the higher-level software (the data path interface) when you disconnect the cable from the ATM module.

If you select Enable, then when you disconnect the cable from the ATM module, the router disables the data path interface after the time you specify with the Data Path Notify Timeout parameter.

If you select Disable, the router does not disable the data path interface when you disconnect the cable from the ATM module.

Instructions: Select Enable or Disable. If you select Enable, be sure to enter an appropriate value for the Data Path Notify Timeout parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.3.2.1.11

Parameter: Data Path Notify Timeout

Path: Configuration Manager > ATM1 > ATM Line Attributes

Default: 1

Options: 0 to 3600

Function: Specifies the time (in seconds) that the router waits before disabling the data path interface when you disconnect the cable from the ATM module, providing that you set the Data Path Enable parameter to Enable.

Instructions: Accept the default or enter an appropriate value.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.3.2.1.12

Parameter: Framing Mode

Path: Configuration Manager > ATM1 > ATM Line Attributes

Default: DS3_CBIT (for DS3 lines) | E3_G832 (for E3 lines) | T1ADM (for DS1 lines) | E1ADM (for E1 lines)

Options: DS3_CBIT | DS3_M32 | T3CBITTPLCP | T3M23PLCP | E3_G751 | E3_G832

Function: Specifies the transceiver mode for the physical interface.

Instructions: Select a transceiver mode as follows:

- DS3_CBIT, DS3_M32, T3CBITTPLCP, or T3M23PLCP for DS3 modules
- E3_G751 or E3_G832 for E3 modules

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.3.2.1.17

Parameter: Cell Scrambling

Path: Configuration Manager > ATM1 > ATM Line Attributes

Default: Off

Options: On | Off

Function: If you select On, the router randomizes cell payload sufficiently to guarantee cell synchronization. If you select Off, cell synchronization problems can occur.

Note that ATM devices with different settings for scrambling cannot communicate. For example, if you configure a router to enable scrambling and configure a hub to disable scrambling, the router and the hub cannot communicate.

Instructions: If you select On, be sure to enable scrambling for all devices on the network. If you select Off, be sure to disable scrambling for all devices on the network.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.3.2.1.22

Parameter:	**Per-VC Clipping**
Path:	Configuration Manager > ATM1 > ATM Line Attributes
Default:	Disable
Options:	Enable | Disable
Function:	Enables or disables cell clipping on a per-VC basis.
Instructions:	Accept the default, Disable, for normal VC clipping. Enable this parameter if you want to clip cells on a per-VC basis.
MIB Object ID:	1.3.6.1.4.1.18.3.4.23.3.1.1.17

Parameter:	**DS3 Line Build Out**
Path:	Configuration Manager > ATM1 > ATM Line Attributes
Default:	Short
Options:	Short | Long
Function:	Conditions router signals to mitigate attenuation, which depends on the physical length of the line. You can set this parameter only for DS3 modules.
Instructions:	Select Short for lines shorter than 225 feet; select Long for lines 225 feet or longer.
MIB Object ID:	1.3.6.1.4.1.18.3.4.23.3.2.1.23

Automated Security Association (IKE) Parameters

You use the following parameters to define a cryptographic key for creating IKE SAs between routers.

Parameter: Pre-shared Key (ascii)

Path: Configuration Manager > Protocols > IP > IKE
Configuration Manager > Edit Circuit > Protocols > Edit IP > IKE

Default: None

Options: Up to 24 ASCII characters

Function: Used as a cryptographic key for creating IKE SAs between routers. IKE is then used to create automated SAs for data packets.

Instructions: Enter an ASCII string, up to 24 characters. Configure the same preshared key on the destination router.

MIB Object ID: None

Parameter: Pre-shared Key (hex)

Path: Configuration Manager > Protocols > IP > IKE
Configuration Manager > Edit Circuit > Protocols > Edit IP > IKE

Default: None

Options: Up to 24 bytes

Function: Used as a cryptographic key for creating IKE SAs between routers. IKE is then used to create automated SAs for data packets.

Instructions: Enter a hexadecimal number, up to 24 bytes. (Enter the prefix **0x** before the digits.) Configure the same preshared key on the destination router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.27.1.1.9

Frame Relay PVC Parameter

You use the following parameter to specify the bandwidth threshold that you want to set for this frame relay PVC.

Parameter:	**Bw Threshold**
Path:	Configuration Manager > Protocols > Frame Relay > Services > PVCs
Default:	0
Options:	0 to maximum physical line speed (bits/s)
Function:	Specifies the bandwidth threshold that you want to set for this PVC for traffic shaping purposes.
Instructions:	To minimize starvation of normal- and low-priority traffic over a high-speed physical line (such as a 56 Kb/s lines over HSSI), set the bandwidth threshold to a value 3 to 10 times that set for the Throughput (CIR) parameter. Otherwise, accept the default, 0.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.2.1.58

IP Global Parameter

You use the following parameter to disable directed broadcast.

Parameter:	**Directed Broadcast**
Path:	Protocols > IP > Global
Default:	Enable
Options:	Enable | Disable
Function:	When this parameter is enabled, a packet addressed to an IP broadcast address goes to all systems on the target network. By default, directed broadcast is enabled. **Caution:** Internet service providers have reported forged ICMP echo request packets sent to IP addresses (SMURF attacks), sometimes resulting in severe network congestion. To prevent these attacks, directed broadcast must be disabled.
Instructions:	Accept the default, Enable, if you want the directed broadcast feature to be enabled. Set to Disable if you want directed broadcast to be disabled.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.1.1.28

IP PIM Parameter

You use the following parameter to determine whether the router interface will act as a PIM bootstrap border interface.

Parameter:	**Bootstrap Border**
Path:	Protocols > IP > PIM > Interface
Default:	Disable
Options:	Disable | Enable
Function:	When you set this parameter to Enable, this PIM interface acts as a PIM bootstrap border interface. A bootstrap border interface discards both incoming and outgoing bootstrap messages. Incoming messages originate from other PIM routers; outgoing messages originate from other PIM interfaces on the same router. When you set this parameter to Disable, this interface operates in accordance with RFC 2362; it accepts incoming messages and forwards outgoing ones.
Instructions:	Set to Enable if you want the interface to discard incoming and outgoing bootstrap messages. Accept the default, Disable, if you want the interface to accept incoming messages and forward outgoing messages.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.14.2.1.32

NAT Global Parameter

The following parameter was used when upgrading from a pre-14.20 NAT configuration to a 14.20 or greater version of BayRS software. This parameter should be set to Enable.

Parameter: Install Private Address

Path: Protocols > IP > NAT > Global

Default: Enable

Options: Enable │ Disable

Function: This parameter was added in BayRS 14.20 to address a compatibility issue concerning non-DNS NAT translations when upgrading from a pre-14.20 NAT configuration to a 14.20 or greater version of BayRS software. This parameter should be set to Enable. Disabling this parameter can cause unpredictable results.

Instructions: Accept the default, Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.1.18

RADIUS Client Parameters

You use the following parameters to configure a RADIUS client. This section replaces “Client IP Address Parameter” in Appendix A of *Configuring RADIUS*.

Parameter: Authentication

Path: Protocols > Global Protocols > RADIUS > Create RADIUS > **Add**

or

Protocols > Global Protocols > RADIUS > Edit RADIUS

Default: Disable

Options: Enable | Disable

Function: Enables or disables the RADIUS client on the gateway.

Instructions: Set to Enable to activate the RADIUS client on the router. Accept the default value, Disable, to deactivate RADIUS authentication.

MIB Object ID: 1.3.6.1.4.1.18.3.5.22.1.1.2

Parameter: Accounting

Path: Protocols > Global Protocols > RADIUS > Create RADIUS > **Add**

or

Protocols > Global Protocols > RADIUS > Edit RADIUS

Default: Disable

Options: Enable | Disable

Function: Enables or disables RADIUS accounting.

Instructions: Set to Enable to activate RADIUS accounting. Accept the default value, Disable, to deactivate RADIUS accounting.

MIB Object ID: 1.3.6.1.4.1.18.3.5.22.1.1.3

Parameter: **Client IP Address**

Path: Protocols > Global Protocols > RADIUS > Create RADIUS > **Add**
or
Protocols > Global Protocols > RADIUS > Edit RADIUS > **Edit**

Default: None

Options: A 32-bit IP address

Function: Identifies the RADIUS client. This address applies to the entire router.

Instructions: Enter the IP address of the router. If the RADIUS server is already configured, Site Manager automatically supplies the address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.22.1.1.5

Parameter: **Debug Message Level**

Path: Protocols > Global Protocols > RADIUS > Create RADIUS > **Add**
or
Protocols > Global Protocols > RADIUS > Edit RADIUS

Default: NODEBUG

Options: ONE | TWO | THREE | NODEBUG

Function: Assigns the level of RADIUS debug messages that the RADIUS client logs.

Instructions: Accept the default value, NODEBUG, unless you are specifically trying to debug the connection.

MIB Object ID: 1.3.6.1.4.1.18.3.5.22.1.1.7

RADIUS Access Control Parameters

You use the following parameters to modify router access.

Parameter: **User Manager Lock**

Path: Protocols > Global Protocols > RADIUS > Access Control

Default: Disabled

Options: Enable | Disable

Function: Allows you to modify access to the router by enabling or disabling the user/manager lock.

Instructions: Set to Enable to lock out the user and manager profile and allow access only by individual users with a unique profile. Accept the default value, Disable, to allow access by all users with the manager or user profile, in addition to users with a unique profile.

Note: If the user/manager lock is enabled and the RADIUS server becomes unavailable, the message "RADIUS wait state" appears in the User Manager Lock field. When the RADIUS server becomes available, the value reverts to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.22.1.10

Parameter: **Login Accounting**

Path: Protocols > Global Protocols > RADIUS > Access Control

Default: Disable

Options: Enable | Disable

Function: Enables or disables login accounting.

Instructions: Set to Enable if you want RADIUS Accounting messages to be sent to the RADIUS server. Accept the default value, Disable, to prevent RADIUS accounting messages from being sent to the server.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.22.1.11

VRRP Parameter

You use the following parameter to enable or disable the VRRP ping feature.

Parameter:	**VRRP Address Ping**
Path:	Protocols > Global Protocols > IP > VRRP
Default:	Disable
Options:	Enable | Disable
Function:	Allows you to ping a master virtual router that is not the owner of the virtual router IP address. This feature is useful for checking network connectivity.
Instructions:	Set to Enable to allow the router to ping a master virtual router that is not the owner of the virtual router IP address. Accept the default, Disable, to prevent that master virtual router from responding to a ping. When this feature is disabled, VRRP is in full compliance with RFC 2338.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.25.1.1.15